العنوان:	صعوبات التحقيق وإثبات الجرائم المعلوماتية قانونا وقضاء وأساليب مواجهتها مع عرض وتقدير تجارب بعض الدول العربية والأجنبية
المصدر:	المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC - كلية علوم الحاسب والمعلومات - جامعة الإمام محمد بن سعود الإسلامية - السعودية
المؤلف الرئيسي:	وسيلة، بوحية
محكمة:	نعم
التاريخ الميلادي:	2015
مكان انعقاد المؤتمر:	المملكة العربية السعودية. الرياض
رقم المؤتمر:	1
الهيئة المسؤولة:	جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات
الشهر:	نوفمبر
الصفحات:	114 - 126
رقم MD:	690615
نوع المحتوى:	بحوث المؤتمرات
قواعد المعلومات:	HumanIndex
مواضيع:	الجرائم المعلوماتية
رابط:	http://search.mandumah.com/Record/690615

صعوبات التحقيق وإثبات الجرائم المعلوماتية
قانوناً وقضاء وأساليب مواجهتها
مع عرض وتقدير تجارب بعض الدول العربية والأجنبية

د. بوحية وسيلة

أستاذة محاضرة بكلية الحقوق والعلوم السياسية

جامعة الجيلالي بونعامة خميس مليانة

الجزائر

Enour44@yahoo.fr

الملخص - تطورت وسائل وأساليب ارتكاب الجريمة بشكل كبير في الوقت الحالي، حيث أبنه وبتطور تكنولوجيا المعلومات والاتصالات ظهر نوع خطير من الإجرام وهو ما يسمى "بالجرائم المعلوماتية" التي أضحت تشكل تهديداً حقيقياً سواء على الأفراد، والشركات، والدول والمجتمعات من كل النواحي الاقتصادية، والاجتماعية، والثقافية وغيرها، والتي لم تسلم منها حتى أكثر الدول تقدماً بالرغم من استخدامها أنظمة عالية جداً لحماية أمن معلوماتها لذلك شغلت الجرائم المعلوماتية بال الحكومات العربية والغربية على حدا سواء، خاصة وأن هذا النوع من الجرائم يتميز بخصوصيات تجعل مسألة تتبع مرتكبيها والتحقيق فيها وإثباتها ومعاقبة مرتكبيها من أكثر الصعوبات التي تواجهها الدول.

وبالرغم من ذلك، فقد بذلت العديد من الدول الغربية كالولايات المتحدة الأمريكية، وروسيا، وكندا و الدول العربية، كالإمارات العربية المتحدة والسعودية جهوداً كبيرة لمكافحة هذا النوع الخطير من الإجرام، حيث قامت بسن قوانين تجرم الأفعال التي تشكل جرائم معلوماتية وتحاول البحث عن وسائل وأساليب حديثة للتحقيق وإثبات هذه الجرائم، خاصة وأن إجراءات التحقيق ووسائل الإثبات المعمول بها في الجرائم التقليدية لا يصلح استخدامها في هذا النوع من الجرائم.

الكلمات المفتاحية: صعوبات التحقيق، إثبات، الجرائم المعلوماتية، قانوناً، قضاء، أساليب مواجهتها.

1- مقدمة

لقد أثبت الممارسة القانونية والقضائية أن الجرائم في تطور مستمر، ومعها تتطور الوسائل القانونية و القضائية لمواجهتها، حتى أصبحت كليات القانون و المعاهد المتخصصة تدرس علم قائم بذاته وهو "علم الإجرام ".

ومهما بلغ مرتكبو الجرائم العادية قدراً من الذكاء، فهي لا تختلف عن الجرائم الأخرى كالجرائم الدولية و المنظمة، وبالتالي ففي الكثير من الحالات يتم التوصل إلى مرتكبيها من خلال تطور أساليب البحث والتحقيق القضائي والإثبات الجنائي، إلا أنه وفي العصر الحالي ظهر نوع جديد من الجرائم يسمى بـ " الجرائم المعلوماتية "، و هي لا تقل خطورة وفتكاً من الجرائم التقليدية، بل أصبحت الجريمة المعلوماتية تشكل تهديداً حقيقياً سواء على الأفراد أو المجتمعات والدول مالياً واقتصادياً، و اجتماعياً وثقافيا ودينياً، ذلك لأن الجناة هم على قدر كبير من المعرفة الفنية ببرامج الحاسب الآلي، وبالتالي تمكنهم هذه المعرفة من ارتكاب جرائم دون ترك آثار تمكن المحققين من الوصول إليهم وتوقيع المسئولية المدنية والجنائية عليهم.

وقد أثبت الواقع وأكدت الحقائق أنه لا يتم اكتشاف إلا واحد بالمائة 1/ 100 من الجرائم المعلوماتية المرتكبة أما تلك التي تم الإبلاغ عنها فلم تتعدى 5/ 100، بل وحتى القضايا التي طرحت على القضاء للفصل فيها فلم يتم الإدانة إلا في حدود الخمس وذلك بسبب عدم كفاية الأدلة وصعوبة إثباتها، على اعتبار أن التحقيق الفني القضائي يهدف إلى جمع الأدلة المادية، في حين أن نظم الحاسوب عبارة عن كيان معنوي لهذا يرى جانب كبير من الفقه القانوني إلى عدم إمكانية تطبيق إجراءات التحقيق الفني التقليدية المنطبقة على الجرائم العادية في جرائم الحاسوب والإنترنت.

والصعوبة التي تعترض التحقيق القضائي وإثبات الجريمة المعلوماتية هي أمر لا يمكن إنكاره غير أن ذلك ليس بمستحيل، لهذا تتجه الجهود سواء على المستوى الوطني والمستوى الدولي إلى إيجاد النصوص والآليات القانونية والقضائية والتي قد تكون فعالة للوصول إلى المجرم الإلكتروني —كما يطلق عليه — وإثبات الجريمة في حقه من خلال وضع القوانين والتشريعات وتعديلها بما يتوافق مع ذلك والاستناد على الوسائل القانونية و الفنية والقضائية الملائمة في البحث والتحري، والتحقيق، والتفتيش والضبط وللوصول إلى المجرم

الإلكتروني و توقيع العقاب الجنائي عليه وعلى هذا الأساس سنحاول التطرق إلى الصعوبات التي تعترض عملية التحقيق و إثبات الجريمة المعلوماتية، من خلال الوسائل القانونية المتاحة بالإضافة إلى أساليب التحقيق القانونية و القضائية، ومنه عرض بعض التجارب للدول الرائدة في هذا المجال مثل الولايات المتحدة الأمريكية وبريطانيا و فرنسا وكندا، وأما على صعيد الدول العربية سنحاول استعراض التجربة السعودية والأردنية والجزائرية في هذا المجال.

وعليه فإن موضوع بحثنا هذا يطرح العديد من الإشكاليات التي تحتاج إلى البحث والإجابة عنها وتتمثل في :

* ما هي السمات المميزة للجرائم المعلوماتية والتي تميزها عن غيرها من الجرائم الأخرى ؟
* وما هي أهم القوانين والتشريعات الوطنية التي نصت على الجرائم المعلوماتية وأساليب البحث والتحقيق فيها ؟
* ما هي طرق وأدلة الإثبات الجنائي للجرائم المعلوماتية في القوانين الوطنية ؟
* ما هي الصعوبات والتحديات التي تواجه عملية التحقيق القضائي في الكشف عن المجرم المعلوماتي أو الإلكتروني ؟
* وما هي تجارب الدول الرائدة في مجال التحقيق و الكشف عن مرتكبي الجرائم المعلوماتية ؟، وهل القوانين الوطنية هي كافية لردع ومكافحة الجرائم المعلوماتية، أم هي مجرد محاولات لا يمكن معها القضاء والحد من هذه الجرائم ؟

وللإجابة على هذه الإشكاليات ارتأينا تقسيم موضوع بحثنا إلى ما يلي :

1) خصوصية الجرائم المعلوماتية وإشكالية التحقيق و الإثبات الجنائي فيها.
2) الصعوبات والتحديات التي تواجه نظم التحقيق وأدلة الإثبات في التشريعات الوطنية.
3) عرض وتقدير تجارب بعض الدول الغربية (أمريكا، فرنسا وبريطانيا وكندا).
4) عرض وتقدير تجارب بعض الدول العربية (السعودية، الأردن، الجزائر).

2- المحور الأول: خصوصية الجرائم المعلوماتية وإشكالية التحقيق و الإثبات الجنائي فيها.

لقد استعمل مصطلح المعلوماتية لأول مرة من طرف "ميكلايلوف – A. I. MIKLAILOV مدير المعهد الإتحادي للمعلومات العلمية والتقنية بالإتحاد السوفيتي سابقاً، وبعدها ذاع استعمال المصطلح على نحو عالمي بشكل واسع حتى أحصى له البعض ثلاثين تعريفاً مختلفاً في الكتابات المتخصصة في علم المعلومات [(1)].

والذي يعنينا في هذا المقام ليس تحديد معنى المصطلح، وإنما الاستعمال السلبي للتقنية المعلوماتية، أو بما يطلق عليه من الناحية القانونية الجريمة المعلوماتية، وما تشكله من تهديد ليس فقط للدولة، بل تعداه ليصبح تهديداً عالمياً، إذ لم تعد الجريمة المعلوماتية جريمة وطنية، بل أصبحت جريمة عبر الوطنية، وقد وصفها الدكتور محمد صالح العدلي. أستاذ القانون الجنائي بكلية الحقوق بمسقط وجامعة الأزهر بمصر بقوله : "الجريمة الإلكترونية هي الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة، أو هي المارد الذي خرج من القمقم ... ولا تستطيع العولمة أن تصرفه ... بعد أن أحضرته الممارسة السيئة لثورة تكنولوجيا المعلومات " [(2)].

وتشير التقديرات أن الجرائم الإلكترونية تكلف دول العالم 400 مليار دولار سنوياً، وتشكل خسائر الولايات المتحدة الأمريكية نحو ربعها، كما كلفت هجمة إلكترونية شركة بريطانية 1.3 مليار دولار، وكذا خسارة مصرفين في الخليج العربي 45 مليون دولار في ساعات قليلة، وبحسب دراسة أجراها مركز الدراسات الإستراتيجية والدولية في واشنطن، يحقق اقتصاد الإنترنيت ما بين " تريليونين وثلاثة تريليونات دولا سنوياً، وهي حصة الاقتصاد العالمي، وأن الجريمة الإلكترونية تستنزف ما بين 15 و 20 بالمائة من القيمة التي تخلقها الإنترنيت [(3)].

وقد أشارت دراسة أن حجم توقعات الجرائم الإلكترونية تتسبب بخسارة دول مجلس التعاون الخليجي ما بين 550 مليون و 735 مليون دولار، وفي دراسة أجرتها شركة نورتن الرائدة في تطوير الحلول البرمجية الأمنية، أن ثلثي مستخدمي الانترنت حول العالم تعرضوا لجريمة إلكترونية على الأقل مرة واحدة، وقد تمثلت في هجمات فيروسية أو تجسسية أو احتيالية لسرقة بطاقات الائتمان وسرقة الهوية أو البيانات المصرفية والشخصية الحساسة، كما أشارت الدراسة إلى أن عملية إزالة الآثار المترتبة من الجريمة الإلكترونية تستغرق في المتوسط 28 يوم كما تكلف في المتوسط 334 دولار [(4)].

وبالنسبة للمجرمين فقد أفقد القرصان كيفين ميتيند – Kevin mitinid – 292 مليون دولار لأربع شركات وهي شركة نوكيا – NOVWELL – SUN – Nokia EC AMERCA وقد صرحت هذه الشركات أنه بمجرد سلب القرصان لجزء من مجموعة الرموز وتصاميم بعض البرمجيات أفقدها عائدات معتبرة.

أما اليوم فتشير التوقعات إلى أن معدل الإنفاق العالمي على تقنية المعلومات سيبلغ 3.5 تريليون دولار خلال العام 2015، أي بتراجع نسبته 5.5 بالمائة عما حققه في العام 2014، وذلك وفقاً لنتائج آخر التقارير الصادرة عن مؤسسة الدراسات والأبحاث العالمية "جارتنر" (5).

وعليه، فالأمثلة كثيرة وكثيرة جداً لا يسعنا المقام للتطرق إليها، وقد أشرنا إلى البعض منها لإبراز حجم الظاهرة، ومن فالجريمة المعلوماتية في ازدياد بشكل لافت وخطير، ومنه نطرح التساؤل التالي: ما هي خصائص الجريمة المعلوماتية ؟

أولاً: تعريف الجريمة المعلوماتية

تعرف الجريمة المعلوماتية من منظور "منظمة التعاون الاقتصادي والتنمية ": "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً، بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية" (6).

وعرفها "مكتب المحاسبة العام" في الولايات المتحدة الأمريكية: "بأنها تلك الأفعال العمدية التي تسبب خسائر للحكومة أو مكاسب للأفراد، والمرتبطة بتصميم، أو استخدام أو تشغيل النظام الذي تقع هذه الأفعال في نطاقه" (7).

ومن الناحية القانونية تعرف الجريمة المعلوماتية بأنها "كل عمل أو امتناع عن عمل أتيه الإنسان إضراراً بمكونات الحاسب الآلي المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي يحميها قانون العقوبات ". أما الأستاذ Mass فقد عرفها بأنها" تلك الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بهدف تحقيق الربح " (8).

أما بالنسبة للمشرع الجزائري فقد نص في المادة 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الصادر عام 2006 على جريمة المساس بأنظمة المعالجة الآلية للمعطيات والبيانات وتتعلق بارتكاب أحد الأفعال التالية بعقوبات متفاوتة :

أ- الإدخال أو الإبقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة القيام بذاك.

ب- تخريب نظم أشغال المنظومة.

ج- القيام عمداً وبطريق الغش بتصميم، أو بحث، أو تجميع، أو توفير، أو نشر، أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

د- حيازة، أو إفشاء، أو نشر، أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

وما يلاحظ أن المشرع الجزائري قد أعطى وصف الجرائم المعلوماتية الجنحة وليس الجناية، غير أنه يعاقب على الشروع فيها بنص صريح ورد في المادة 394 مكرر 7.

ثانياً: خصائص الجريمة المعلوماتية :

تمتاز الجريمة المنظمة بميزات وخصائص تميزها عن غيرها من الجرائم التقليدية، وتتمثل خصائص الجريمة المعلوماتية فيما يلي:

أ- خطورة الجريمة المعلوماتية : حيث تمس الحياة الخاصة للإنسان، كما أنها تمس أمن ولاسيما منها المؤسسات العامة والخاصة منها البنوك والمصارف التي أصبحت مستهدفة معلوماتياً كما أنها تستهدف أمن الدول وتمس باقتصادياتها، وقد يصل الأمر إلى التأثير على الجانب السياسي فيها، وذلك عندما تيتم تسريب البيانات والمعلومات الخاصة بها ونشرها أو تخريب أنظمة تشغيل المعلومات الخاصة بها.

2- عالمية الجريمة المعلوماتية "جرائم عابرة للحدود الوطنية" : لم تعد الجريمة المعلوماتية جريمة وطنية، بل تعدت الأوطان للتجاوز حتى القارات، ويعود السبب في هذا إلى انتشار شبكة الاتصالات العالمية " الإنترنت "، بحيث أصبحت الحواسيب في كل أرجاء العالم مربوطة بهذه الشبكة، وبالتالي يمكن للجاني أن يكون من جنسية دولة ما، ويرتكب جريمة إلكترونية باستعمال حاسب آلي في دولة أخرى قصد إحداث ضرر في دولة ثالثة، وبهذا تقع الجرائم في أغلب الأحيان عبر حدود دولية. (9)

3- صعوبة إثباتها : على عكس الجرائم التقليدية التي يترك فيها الجاني دليل للوصول إليه أو عن طريق التحقيق والتحري يمكن الوصول إلى حل لغز الجريمة، و الوصول والقبض على مرتكبيها فالجريمة الإلكترونية صعبة الإثبات لأنا لا تترك دليلاً خارجياً، حيث أن هذه الجرائم ما هي في حقيقتها إلا نبضات إلكترونية، فإن هذا الشكل عقبة كأداة أمام اكتشافها، وأمام التعرف على مرتكبيها، ولاسيما أن هناك صعوبة في تعقب آثار تلك الجرائم وتعقب مرتكبيها (10).

كما ترجع صعوبة إثباتها لأسباب أخرى نذكر منها :
- أنها جريمة لا تترك أثراً بعد ارتكابها.
- صعوبة الاحتفاظ الفني بآثارها إن وجدت.
- أنها تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها.
- أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
- أنها تعتمد على قمة الذكاء في ارتكابها، فالمجرم على قدر كبير من المعرفة الفنية ومن الذكاء [11].

4- هي جرائم لا تعتمد على العنف : على عكس الجريمة التقليدية التي تحتاج إلى جهد بدني في ارتكابها مثل السرقة والاغتصاب، فإن الجرائم المعلوماتية توصف بالجرائم الناعمة، أو جرائم الذكاء، بحيث أنها تقوم على الدراسة الذهنية والتفكير العلمي المدروس القائم على دراية ومعرفة كبيرة بالحاسب الآلي كما أن أغلب المجرمين ذوي مستوى تعليمي عالي [12].

5- هي جرائم تعتمد على وجود الحاسب الآلي و على معرفة جيدة بأنظمة التشغيل وتقنيات المعلومات، كما أن الأشخاص مرتكبيها فهم أشخاص من دوي الخبرة والذكاء في هذا المجال.

3- المحور الثاني: الصعوبات والتحديات التي تواجه نظم التحقيق وأدلة الإثبات في التشريعات الوطنية

لقد ألف المشتغلون في المجال القانوني و القضائي التعامل مع المفاهيم التقليدية في التحقيق و تقديم أدلة الإثبات الجنائية، وبالرغم من أن أدلة الإثبات قد أصبحت تعتمد على التقنية وغيرها من الوسائل الحديثة، إلا أنها في مجال الجريمة المعلوماتية غير كافية، وذلك بالنظر إلى التطور الكبير والسريع الذي يشهده عالم المعلوماتية، ومن الصعوبات التي تعترض عمليات التحقيق والتحري في الجرائم المعلوماتية مذكر ما يلي:

أولاً: عدم ظهور الدليل المادي وعدم تركه : يعتبر عالم الشبكة العنكبوتية عالم افتراضي، وبالتالي في مكن بضغطه زر تغيير الكثير من المعلومات في وقت قصير، فيصعب استخلاص الدليل المادي لهذه الجريمة، لأنه بكل بساطة في عالم غير واقعي.

وبالإضافة إلى هذا فيعمل المجرم على التخطيط الجيد من أجل عدم ترك دليل مادي حتى وإن تركه، فإنه بإمكانه العودة مرة ثانية ومحوه قبل وصول يد القضاء إليه [13].

ثانياً: عدم الإبلاغ عنها للسلطات المختصة في الدول : يعتبر من أحد الأسباب الرئيسية لعدم ضبط مجرمي المعلوماتية هو عدم التبليغ على هذه الجرائم سواء من طرف الأفراد أو من الشركات بسبب الخوف على السمعة التجارية، أو الاعتقاد بأن هذا التبليغ يعتبر محفزاً لمجرمين آخرين للهجوم عليها مرة ثانية على اعتبار أن النظام المعلوماتي لهذه الشركة يحتوي على ثغرات أمنية.

ثالثاً – نقص الخبرة في تتبع الجريمة وتحديد طرق ووسائل وزمان ارتكابها : إن وتيرة ارتكاب الجريمة المعلوماتية سريعة جداً، كما أن المجرمين على قدر كبير من الذكاء والمعرفة الفنية بالحاسب الآلي، الأمر الذي لا يتوافر لدى المحققين، مما يضعنا أمام أجهزة غير متكافئة [14]. وقد وصل ببعض مجرمي المعلوماتية الإطلاق على أنفسهم اسم النخبة، أما رجال الشرطة فقد أطلقوا عليهم اسم الضعفاء.

وفي دراسة أجريت في لإنجلترا عام 1986، وشملت 195 حالة من حالات الاحتيال لاختلاس المال عن طريق الحاسب الآلي، 15 % منه قد تم اكتشافها مصادفة، في حين أن 15 % منها قد تم اكتشافه نتيجة يقظه المدققين، والمراجعين الداخلين والخارجين حيال قيامهم بأعمال التدقيق الروتينية 16 % منها اكتشفت بفضل دقة عمل الإدارة، 10 % منها على شكوى المجني عليه، 7 % على أثر تغيرات في القيادة الإدارية، و 3 % لأسباب تتعلق بتغير نمط حياة الجاني [15].

ولهذا يميل الفقه الجنائي إلى القول بضرورة تنمية الخبرة والمهارات للأشخاص المتخصصين لوضع مناهج للتدريب على التحقيق وإثبات الجرائم المعلوماتية، مراعين في هذا خصوصية التطور التقني السريع.

والخبرة المطلوبة من أجل إثبات هذه الجريمة يجب أن تكون من نوع خاص يتماشى وخصوصية الجريمة، وقد تعمل بعض البلدان على إعادة تأهيل بعض ما يسمى بالمجرمين المعلوماتيين من أجل الاستفادة من خبراتهم في الاختراق والقرصنة.

وبالنسبة للتحديات التي تواجه تشريعات الدول العربية، ليس كل الدول العربية تعير اهتماماً لهذه الجرائم المستحدثة، لكن واضح أن دول المشرق على رأسها مصر، والأردن، ولبنان ودول الخليج المتمثلة في الإمارات العربية المتحدة تولي اهتماماً بالغاً لهذه الجرائم.

ففي مصر تم لأول مرة إنشاء إدارة عامة لمكافحة جرائم الحاسب الآلي وشبكة المعلومات فرجال الشرطة المصرية يتلقون تكويناً في مجال مكافحة الجريمة المعلوماتية، والتي أفشلت عدة محاولات لسرقة بطاقة الائتمان عن طريق الإنترنيت، التي قام بها شباب جامعي، وكذا تم القبض على مهندس قام بإنشاء موقع لتشويه سمعة بنت رجل مصري مهم عن طريق الإنترنت.

أما في الأردن، فيعمل محاموها على مواكبة التطور والاختصاص في مجال المعلوماتية ومن بينهم الأستاذ "يونس عرب" الذي أصدر كتاباً في مجال الكمبيوتر والإنترنت.

وقد صادقت تونس والأردن على اتفاقية تسمح بإمكانية استخدام التوقيع الإلكتروني، مما يفتح آفاق واسعة أمام معاملات إلكترونية جديدة، وقد أصدرت تونس قانون 2001 فحواه أن العقد الإلكتروني تسري عليه نفس أحكام العقد العادي فيما لا يخالف القواعد الآمرة في القانون أنه جاء من دول أي تفصيل.

وأما الرائدة في هذا المجال، فهي دولة الإمارات العربية المتحدة حيث قامت بسن قانون مكافحة جرائم تقنية المعلومات عام 2006، حيث يعاقب هذا القانون بعقوبة السجن المؤقت وبعقوبتي الحبس أو الغرامة أو بكلاهما معاً عن كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به، وترتب على الفعل إلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو إعادة نشر بيانات، أو معلومات.

وعملت على تدريب عناصر الشرطة من أجل التعامل مع هذه السلوكيات، كما أنها قريباً ستصدر قانون التجارة الإلكترونية والأهم من هذا سوف تصدر قانون مكافحة الجريمة الإلكترونية [16].

وعلى هذه الدول المتبقية مواكبة التطورات و مراعاة اختلاف البيئة التي تتم فيها المعاملات الإلكترونية عن المعاملات العادية لأن اختلاف الافتراضي عن الواقعي هو حقيقة، كما أنه يجب على الدول العربية اعتماد الوسيلتين التاليتين، كوسائل للتحقيق والاستدلال و إثبات الجريمة المعلوماتية، وهي الخبرة والمعاينة.

وفي هذا الشأن، نقول بأنه يجب أن يتوفر الخبير على مؤهلات عالية، ومقدرة فنية وخصوصاً: [17]

1- يجب أن يعرف تركيب الكمبيوتر.

2- معرفة شاملة لشبكة الإنترنت.

3- التعامل مع الجريمة التي خلفتها الجريمة.

4- كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف.

رابعاً: صعوبة إجراء المعاينة ونقص الكفاءة البشرية والوسائل العلمية والتقنية للقيام بها : قد يكون الحل في بعض أنواع الجرائم الإلكترونية، ولتكون المعاينة لابد من وجود مسرح الجريمة، وهذا ما يصعب تحديده وبالتالي صعوبة الحفاظ على الآثار المادية هذا إن وجدت، وقد يكون الفارق الزمني بين حدوث الجريمة و اكتشافها أو التحقيق فيها كبير ومن أجل المعاينة لابد من التبليغ والشخص المبلغ له يجب أن يكون عالماً بالتقنية من أجل التحفظ على الأدلة إن وجدت.

4- المحور الثالث : عرض وتقدير تجارب بعض الدول الغربية (أمريكا، فرنسا وبريطانيا وكندا)

اتجهت كافة الدول المتقدمة تكنولوجيا إلى استحداث نصوص قانونية جديدة تجرم الجرائم الإلكترونية الجديدة على قوانينها القديمة التقليدية، وصاغت نصوص قانونية جديدة قادرة على التعامل ومواجهة هذا النوع من الجرائم المتطورة تكنولوجيا [18].

وتعد السويد أول بلد سن تشريعات خاصة بجرائم الحاسب الآلي والإنترنيت، حيث صدر قانون البيانات السويدي عام 1973، والذي عالج قضايا الاحتيال عن طريق الحاسب الآلي زيادة على شمول فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويدها، أو تحويلها، أو الحصول غير المشروع عليها [19].

وقبل عرض تجارب الدول الغربية في مجال مكافحة الجرائم المعلوماتية، فإننا أعددنا جدولاً نبين فيه الدول قائمة الدول الغربية الأكثر تعرضاً للهجمات الإلكترونية وفقاً لتحقيق أعده فريق "البوصلة" بعمان الأردن استناداً إلى إحصائيات رسمية حصلت عليها، ودراسة أعدتها شركة "كاسبرسكي لاب" الروسية المتخصصة في أمن الحواسيب ومكافحة الفيروسات عام 2013 [20].

الدول الغربية الأكثر تعرضاً للهجمات الإلكترونية في العالم	النسبة المئوية	المرتبة
الولايات المتحدة الأمريكية	% 30.80	1
روسيا	% 11.20	2
ألمانيا	% 9.32	3
اليابان	% 6.24	4
بريطانيا	% 5.20	5
الهند	% 4.08	6

وعليه سنحاول في هذا المحور التطرق إلى تجارب بعض الدول الغربية لمواجهة الجريمة المعلوماتية.

أولاً – تجربة الولايات المتحدة الأمريكية : تعتبر الولايات المتحدة الأمريكية مهد التقنية المعلوماتية والشبكة العنكبوتية، فهي دولة رائدة ومتقدمة جداً في مجال المجتمع المعلوماتي، ولكنها بالمقابل من أكثر الدول تعرضاً للهجمات الإلكترونية، فقد أعلن مكتب التحقيقات الأمريكي – FBI – أن جميع الشركات الكبرى (500 شركة) تعرضت لهجوم عبر الإنترنيت، وأنه في عام 2004 مثل الاحتيال عبر الإنترنيت نسبة 32 من مجموع شكاوي المستهلكين لدى لجنة التجارة الاتحادية، كما أن أنفقته مؤسسات الأعمال لمكافحة المخربين والفيروسات تجاوز 300 مليار دولار في عام 2000 [21].

وقد شرعت الولايات المتحدة الأمريكية في إصدار قوانين خاصة تجرم الجرائم الإلكترونية، حيث شرعت قانون خاص لحماية أنظمة الحاسب الآلي الفيدرالي، يعد ما تبلور جهد لجنة الكونجرس بإصدارهم مشروع القانون، و أطلق عليه قانون الإحتيال وإساءة استخدام الحاسب الآلي – The computer Fraud and abuse Act – وقد تم تعديل هذا القانون عام 1986 و 1994، وفي عام 1986 صدر قانوناً يحمل الرقم 1213 عرف كافة المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية، ووضعت المتطلبات اللازمة لتطبيقه [22].

وفي فيفري 1996 قام الرئيس الأمريكي "بيل كلنتون" بالتوقيع على قانون الاتصالات، والذي استهدف تقييد حرية القصر في الإطلاع على الصور والمواد المخلة بالآداب، إلا أن هذا القانون تم إلغاءه من المحكمة الدستورية الفيدرالية [23].

وفي ديسمبر عام 1997 وقع الرئيس كلينتون على قانون السرقة غير الإلكترونية – The No Electronic Theft – بالقرار (H. R 2265)، وجاء "قانون النيت" من أجل تعزيز حماية حقوق الطبع والعلامات التجارية، ومن أجل تعديل النصوص الواردة في القانون الفيدرالي رقم 18 والقانون رقم 17 [24].

وهناك أحكام صدرت على القضاء الأمريكي فيما يتعلق باختصاص بالنظر والفصل فيها في حالة تنازع الاختصاص المكاني مع قضاء دولة أخرى، حتى ولو ترتكب الجريمة على أقاليمها تطبيقاً لمبدأ الشخصية هذا الأخير بالنظر في الجرائم الإلكترونية أو المعلوماتية وقد أشارت التطبيقات القضائية إلى أنه يكفي لامتداد ولاية القضاء المذكور إلى جريمة وقعت في الخارج أن تكون آثارها قد مست مصالح أمريكية أو عرضتها للخطر، تأسيساً على مبدأ الاختصاص الشخصي، ومثال ذلك ما قضت به المحكمة العليا لولاية " نيويورك " بصدد جريمة انتهاك قانون المستهلك والدعاية الخادعة، وطبق المبدأ ذاته كان قد طبق في قضية أخرى مؤداها قيام إحدى الشركات بولاية " بنسلفانيا" بالادعاء على أحد مزودي الإنترنت في ولاية كاليفورنيا بدعوى الاعتداء على علامة مسجلة في الولاية الأولى، وقد أسست المحكمة حكمها على أن قضاء " بنسلفانيا" ينعقد له الاختصاص الشخصي على اعتبار أن مزود خدمة الإنترنت له مشتركون في الولاية [25].

وبذلك نستخلص أن القانون الأمريكي يتسع نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحققت في الولايات المتحدة الأمريكية، ففي الولايات المتحدة الأمريكية يجيز القانون اعتراض الاتصالات الإلكترونية بصفة عامة بما في ذلك شبكات الحاسب الآلي، وذلك متى تم بإذن من المحكمة.

وبشأن التفتيش عن الجرائم المعلوماتية فإن في الولايات المتحدة الأمريكية تجيز وفقاً للمادة 41 (a) من قانون الإجراءات الجنائية الفيدرالي الأمريكي لقاضي التحقيق إصدار إذن تفتيش ملكية داخل منطقة أو خارجها، متى كانت الملكية عند طلب الإذن موجودة داخل المنطقة، ولكن يخشى أو يتوقع تحركها خارج المنطقة قبل تنفيذ الإذن، وربما المشكلة التي تواجه رجال الضبط عند تنفيذهم التفتيش أنه لا يكون باستطاعتهم التحقق من أن البيانات المضبوطة جرى تخزينها داخل المنطقة أم خارجها [26].

والجدير بالذكر في هذا المقام أن المحاكم الأمريكية درجت على رفض دعاوى بطلان الدليل في حالة عدم استطاعة رجال الضبط معرفة ما إذا كان تنفيذ التفتيش يشكل انتهاكاً للمادة (41) قانوناً أو فعلياً ما لم يتعمد هؤلاء عدم إعمال القاعدة المذكورة، أو أن يكون لديهم حدس مسبق.

وتجدر الإشارة في هذا الصدد أن تنفيذ إذن التفتيش يثير بعض المشكلات في مجال الجرائم المعلوماتية في القانون المذكور، ففي هذا القانون مبدأ يجب أن يلتزم به رجال الضبط القضائي، ألا وهو ضرورة الإعلان عن وجودهم والإفصاح عن السلطات المخولة لهم (أو ما يعرف بقاعدة الاستئذان والإعلان). بيد أن هذه القاعدة العامة يمكن التحلل منها وعدم الالتزام بها علي حد تعبير المحكمة الفيدرالية الأمريكية العليا متى كان مأمور الضبط القضائي قد توافر لديه شك مبرر في أن إعمال هذه القاعدة أو التقيد بها سيكون غير مجد أو من شأنه إعاقة فعالية التحقيق، أو من المتوقع أن تنجم عنه خطورة ما.

ثانياً – تجربة فرنسا: تعتبر فرنسا من الدول المتقدمة في مجال استخدام المعلومات في أوروبا، وقد سعت فرنسا إلى تطوير منظومتها القانونية لمواجهة الجرائم الإلكترونية، حيث صدر قانون خاص عام 1988 يعدل قانون العقوبات الفرنسي، وأضاف جرائم جديدة الحاسب الآلي والعقوبات المقررة لها، حيث تم تجريم غش الحاسب الآلي، وفي عام 1994 تم مرة ثانية تعديل قانون العقوبات ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية، حيث خصص الفصل الثالث من الكتاب الثالث منه بجرائم الاعتداء على نظم المعالجة الآلية للبيانات [27].

كما أقر المشرع الفرنسي حماية جنائية خاصة لبطاقة الائتمان بموجب القانون رقم 1383 – 91 المؤرخ في 30 / 12/ 1991 حيث تم النص على ثلاث جرائم تتعلق بالبطاقات الائتمانية وهي تقليد أو تزوير بطاقة وفاء وسحب، استعمال، أو محاولة استعمال لبطاقة وفاء أو سحب مقلدة، أو مزورة مع العلم بذلك، وكذلك وجوب مصادرة و تدمير البطاقات المقلدة ومصادرة الأدوات التي استخدمت أو المعدة للاستخدام في التزوير أو التقليد، إلا إذا استخدمت بدون علم مالكها.

ففي فرنسا، فإن اختصاصها القضائي في الجرائم المعلوماتية يمتد إلى تلك الجرائم التي وقعت في الخارج عملاً بقانون العقوبات الجديدة، متى كانت الظروف الواقعة تبرر مصلحة فرنسا في إعمال قانونها عليها.

فبشأن التفتيش عن الجرائم الإلكترونية فقد سمح بامتداد التفتيش إلى الحواسيب الموجودة خارج إقليم الدولة، التسهيل عمل سلطات الضبط والتحقيق. وهذا الاتجاه أخذ به القانون الفرنسي من خلال المادة (17) من قانون الأمن الداخلي الفرنسي [28].

ثالثاً – تجربة بريطانيا: تأتي بريطاني كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي، حيث أقرب قانون مكافحة التزوير والتزييف عام 1981، والذي شمل في تعريفاته الخاصة تعريف أداة التزوير ووسائط التخزين الحاسوبية المتنوعة [29].

كما صدر في المملكة المتحدة قانون حماية البيانات – Data Protection – في العام 1984 وفي هذا القانون تم تنظيم العملية القانونية الخاصة بتخزين البيانات الشخصية واسترجاعها بما يتفق ومبادئ اتفاقية مجلس أوروبا لعام 1981 [30].

كما تبنى القضاء الإنجليزي حلولاً مشابهة، فهو يختص بنظر الدعاوي الناشئة عن إساءة استخدام الإنترنت، متى كان ثمة ارتباط بين الواقعة المرتكبة وبريطانيا عملاً بقانون إساءة استخدام الحاسوب الصادر سنة، 199 (The Computer Misuse Act of 1990). فلكي ينعقد الاختصاص للمحاكم الإنجليزية، يكفي امتداد آثار الواقعة إلى بريطانيا، ولو كانت هذه الواقعة قد حدثت في الخارج، وبصرف النظر عن محل إقامة الجاني. بعبارة أخرى، يكفي أن يكون ناتج عمله أو أن نيته منصرفة إلى أن يكون ناتج عمله تعديلاً محظوراً في حاسوب موجود في بريطانيا [31].

وفي هذا الصدد نشير إلى أن شركة بريطانية تكبدت خسائر بلغت 1.3 مليار دولار بسبب هجوم الكتروني واحد، وخسارة مصرفين في الخليج 45 مليون دولار في ساعات قليلة، وإعلان الهند عن تعرض 308371 موقعاً الكترونياً للاختراق بين العامين 2011 و 2013 [32].

رابعاً – التجربة الكندية: بحكم قرب كندا من الولايات المتحدة الأمريكية، تعتبر كندا دولة متقدمة في مجال استخدام المعلومات والحاسب الآلي، لهذا نجدها أنها وضعت منظومة قانونية متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلية والإنترنيت، وقد تجسد هذا عام 1985 من خلال تعديل في قانون العقوبات الكندي، بحيث شمل القانون الجديد تحديد الجرائم المتعلقة بالحاسب الآلي كالدخول غير المشروع لأنظمة الحاسب الآلي، كما جاء في قانون المنافسة تخويل مأموري الضبط القضائي متى حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها.

وكما أصدرت مقاطعة "كيبك Québec " عام 1994 تشريع شامل للخصوصية، وقد قدم هذا القانون مشروع حماية شاملة للبيانات الشخصية في القطاع الخاص [33].

5- المحور الرابع: عرض وتقدير تجارب بعض الدول العربية (السعودية الأردن، الجزائر).

تختلف حجم الجرائم المعلوماتية في الوطن العربي من دولة لأخرى، وهذا راجع إلى الظروف الداخلية في كل دولة، وكذا مدى الاعتماد على الآلة الحاسبة في تسيير الشؤون العامة للدولة أو حتى الشؤون الخاصة للأفراد، وقد أكد خبير اقتصادي أن معدل الجرائم الإلكترونية في العالم يصل إلى 57.6 % حيث يكلف الاقتصاد العالمي ما يقارب 12.950 مليار دولار، وقال أن نسبة معدل الهجمات الإلكترونية في السعودية يقارب 45.8 % كما كانت نسبة الهجمات للحسابات البنكية للأفراد عام 2009 بلغت 40 %، واختراق المواقع الإلكترونية لعام 2009 بلغت 40 %، ورسائل الاحتيال في المملكة لعام 2009 بلغت 43.7 % [34].

وفي دراسة أجرتها شركة " تريند مايكرو" المشهورة بمحاربة الفيروسات أشارت أن المملكة العربية السعودية والإمارات العربية تتصدر المركز الأول والثاني على مستوى دول مجلس التعاون الخليجي وفي السعودية فقط حصل انهيار 700 ألف نظام معلوماتي خلال 9 أشهر [35].

وتحاول العديد من الدول العربية مواكبة التطورات الحاصلة في مجتمع المعلوماتية، وكذا التصدي للآثار السلبية لهذه الظاهرة من خلال وضع منظومة قانونية حديثة وفعالة، وفي هذا السياق سنتطرق إلى كل من تجربة المملكة العربية السعودية، والأردن، والجزائر.

وقبل عرض تجارب الدول العربية في مجال مكافحة الجرائم المعلوماتية أعددنا جدولاً آخرا نبين فيه قائمة الدول قائمة الدول العربية الأكثر تعرضاً للهجمات الإلكترونية وفقاً لتحقيق أعده فريق "البوصلة" بعمان الأردن استناداً إلى إحصائيات رسمية حصلت عليها، ودراسة أعدتها شركة "كاسبرسكي لاب" الروسية المتخصصة في أمن الحواسيب ومكافحة الفيروسات عام 2013 [36].

المرتبة	النسبة المئوية	الدول العربية الأكثر تعرضاً للهجمات الإلكترونية في العام
1	38.08 %	الإمارات العربية المتحدة
2	29.31 %	السعودية
3	10.16 %	مصر
4	9.64 %	قطر
5	6.29 %	الكويت

أولاً – تجربة المملكة العربية السعودية : لقد أسلفنا الذكر أن المملكة العربية السعودية تعاني من كثرة الهجمات الإلكترونية، ولعل الهجمات التي طالت شركة "أرامكو" النفطية أصدق دليل على مدى الخطر الذي يتهدد المملكة حكومتاً وشعباً، وهذا ما استدعى وجوب وضع منظومة قانونية كفيلة بحماية المؤسسات والأفراد وتعقب المجرمين ومحاكمتهم في حالة إمكانية ذلك، وبالفعل فقد وافق مجلس الوزراء في المملكة عام 2007 على نظامي مكافحة جرائم المعلوماتية والتعاملات الإلكترونية، وذلك من أجل وضع حد من وقوع الجرائم المعلوماتية وتحديد الجرائم المستهدفة بالنظام و العقوبات المقررة لكل جريمة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات على مجرمي المعلوماتية.

وكما يهدف هذا القانون إلى تأمين استخدام أجهزة الكمبيوتر وشبكة الإنترنيت من عبث الأفراد والمنظمات الإجرامية وغيرها، والذي يتمثل في ارتكاب جرائم الأموال وجرائم الآداب وجرائم الإرهاب وجرائم السب والقذف وجرائم غسيل الأموال [37].

وعرف نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم م / 17 وتاريخ: 8/ 3/ 1428 هـ بناء على قرار مجلس الوزراء رقم: (79) وتاريخ: 7/ 3/ 1428 هـ الجريمة المعلوماتية بأنها : (أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام).

وكذلك جاء في نص المادة (13) من نظام مكافحة الجرائم المعلوماتية السعودي: (مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها، كما يجوز الحكم بإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه)، وفي هاتين المادتين إشارة إلى صعوبة إثبات مثل هذه الجرائم – وهذا واقع الأمر، ولذلك عبر المقنن بقوله : وكانت الجريمة قد ارتكبت بعلم مالكه ففيه إشارة إلى جهالة الفاعل الأصلي وصعوبة تعيينه، ثم إذا توصل إليه بطرق الإثبات العامة المتقدم ذكرها؛ فإنه بعينه يقع تحت طائلة هذه المواد العقابية.

كما نصت المادة (14) من هذا النظام على: تعاون هيئة الاتصالات وتقنية المعلومات على: تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة.

ثانياً – التجربة الأردنية : تعتبر الجرائم الإلكترونية من الجرائم المصنفة حديثاً خاصة في الأردن، حيث استحدثت الأجهزة الأمنية في العام 2008 ما يسمى " شعبة المتابعة والتحقيق " الخاصة بالجرائم الإلكترونية والتي أدرج تحتها أقساماً متخصصة، تشمل (قسم الإسناد الفني) المعنى بالتحقيق هذه الجرائم، كما أصدرت قانون "جرائم أنظمة المعلومات " منذ العام 2010، وتجدر الإشارة على أن العام الماضي شهد 1300 جريمة إلكترونية وفقاً لبيانات إدارة البحث الجنائي.

وتسعى الأردن لإنشاء مركز وطني للاستجابة لحوادث الكمبيوتر من خلال مركز تكنولوجيا المعلومات الوطني الذي يعتبر مرجعية لأمن وسلامة المعلومات والشبكات، واستناداً بيانات وإحصائيات رسمية أظهرت أن قسم الجرائم الإلكترونية في إدارة البحث الجنائي بمديرية الأمن العام تعاملت العام الماضي مع 1300 جريمة إلكترونية و 400 أخرى العام الحالي، إذ كان 75 في المائة من الضحايا من النساء، وشملت الاحتيال الإلكتروني والابتزاز وتحويل مبالغ مالية ضخمة لحسابات بنكية تابعة لمحتالين خارج البلاد، مع عدم وجود إحصاءات دقيقة بما يتعلق بالخسائر المالية [38].

وقبل أن تصدر الأردن قانون "جرائم أنظمة المعلومات" منذ العام 2010 كانت النصوص القانونية الخاصة بالجرائم المعلوماتية تستمد من أحكام قانون العقوبات الأردني لمكافحة جرائم الإنترنيت والحاسب الآلي، ولمواجهة هذه المشكلة قامت الأردن الإحاطة بهذه الجرائم من خلال ما يلي:

- إصدار قانون حماية حق المؤلف.
- تحديث القوانين السائدة إلى قوانين جديدة تجرم جرائم المعلوماتية.
- الانضمام إلى المعاهدات والاتفاقيات الدولية التي تعمل على تجريم جرائم الإنترنيت.
- استحداث قوانين جديدة تقنن الاستخدامات الإلكترونية مثل قانون المعاملات الإلكترونية.
- إنشاء إدارات جديدة لوزارة الاتصالات تكون مسئولة عن تلك الجرائم [39].

ثالثاً – التجربة الجزائرية : لا شك في أن الجزائر ليست في منأى عن الجرائم المعلوماتية، وأن كان حجم الخسائر المادية غير معروف ومقدر، إلا أنه ليس بحجم الخسائر التي تتكبدها الدول الغنية والمتطورة، ولعل السبب يعود إلى أن الاعتماد على الحاسب الآلي ليس بالكلي، ولا يشمل القطاعات فعلى سبيل المثال تكاد تكون التجارة الإلكترونية في الجزائر غير موجودة من الناحية الفعلية، على اعتبار أن قطاع البنوك لم يتم تحديثه لكي يضمن و يساير هذه العملية.

وقد أضحت الجرائم المعلوماتية من بين اهتمامات الجزائر نتيجة تقارير المنظمات والهيئات الدولية حول الجرائم الإلكترونية وحماية الإنترنيت بحكم أن التقارير الأخيرة كشفت أن الجزائر في المراتب الأولى بالنسبة للقرصنة إفريقيا وعربياً بنسبة 85 بالمائة في مجال القرصنة، وكانت الجزائر ضمن مجموعة الدول المدرجة في مشروع إعداد بحث لتحديد آلية تطور الهجمات الإلكترونية خلال السنوات الثمانية المقبلة من طرف منظمة " التحالف الدولي لحماية أمن الإنترنيت "، والذي يتضمن قديم إرشادات لحكومات الدول والسلطات المحلية حول أفضل السبل المتاحة لمواجهة هذه الهجمات، غير أنه وفي المقابل لا يوجد قانون مستقل وموحد يعالج مختلف الجرائم المعلوماتية والعقوبات المقررة لها.

وبالرغم من ذلك نشير أن هناك جهود كبيرة تبذل من طرف الدولة الجزائرية لتحديث الإدارة وتمكين المواطن الجزائري من استعمال وسائل الاتصال الحديثة و توفير الإنترنيت الأمر الذي انعكس على عدد مستعملي الإنترنيت فهو بتصاعد مستمر، بالإضافة إلى إطلاق شبكة الجيل الثالث من الهواتف النقالة التي تتيح استعمالاً شخصياً للإنترنيت وبتدفق عالي السرعة، ولكن بالمقابل، فإن هناك تزايد لنسب الجرائم المعلوماتية بمختلف صورها الأمر الذي جعل الدولة الجزائرية تتخذ مجموعة من الإجراءات لمكافحة هذه الجرائم الجديدة على المجتمع الجزائري، وتتمثل فيما يلي:

1- في نوفمبر 2008 تم إبرام اتفاق تعاون أمني بين الجزائر وباريس، يشمل تتبع الجرائم المعلوماتية على شبكة الإنترنيت التي تديره شبكات توصف نفسها بالجهادية.

2- إنشاء مركز لمكافحة الجريمة الإلكترونية بالجزائر العاصمة بدائرة بئر مراد رايس بتاريخ 18/ 05/ 2008، وكذا إنشاء معهد خاص بعلم الإجرام، وتهدف هذه الهيئات على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادي أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في البيوت والبنوك، وأضاف المتحرك أن مركز مكافحة الجريمة المعلوماتية يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى (40).

3- وفي عام 2009 صادق البرلمان الجزائري على مشروع القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد تضمن هذا القانون 19 مادة موزعة على 6 فصول تم إعداده من نخبة من رجال القانون وبمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاماً خاصة بالمراقبة الإلكترونية التي لا يجوز إجراءها، إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها، وهي الأفعال الموصوفة بجرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة، أو حالة توفر معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام، وينص القانون أيضاً على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال، ومكافحته تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المعلوماتية، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفل اللجنة أيضاً بتبادل المعلومات مع نظيراتها في الخارج، علماً أن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل (41).

وفي هذا الصدد نشير إلى أن مصالح المديرية العامة للأمن الوطني تمكنت عام 2013، من معالجة أكثر من 380 قضية تتعلق بالجريمة الإلكترونية خلال السداسي الأول من سنة 2013 حسبما علم اليوم، من هذا السلك الأمني، وتم التأكيد خلال معرض حول تكنولوجيات الإعلام والاتصال نظم على هامش الاجتماع الـ 2 للمنتدى العربي حول تسيير الإنترنت شاركت فيه المديرية العامة للأمن الوطني أنه قد تم خلال السداسي الأول من سنة 2013 معالجة ما مجموعة 383 قضية تتعلق بالجريمة الإلكترونية في حين تم معالجة 515 قضية خلال السنة الماضية، و يتعلق الأمر بـ 126 قضية خاصة بالاستغلال غير القانوني للأداة المعلوماتية و 154 تتعلق بالهاتف النقال، و 103 تخص الصور الفوتوغرافية والفيديو في هذا الصدد عالجت الخلية المركزية لمكافحة الجريمة الإلكترونية العديد منها عام 2012 (42).

وفيما يتعلق بقانون الجرائم المعلوماتية، فقد نص المشرع الجزائري في المادة 394 مكرر إلى 394 مكرر إلى مكرر 7 من قانون العقوبات لعام 2006 على جريمة المساس بأنظمة المعالجة الآلية للمعطيات والبيانات، و قرر لها عقوبات متفاوتة (43).

ولم يضع قانون مستقل وخاص بمكافحة الجرائم المعلوماتية في الجزائر صرح رئيس اللجنة الوطنية لترقية وحماية حقوق الإنسان، صعوبة تطبيق القوانين المعاقبة على الجريمة الإلكترونية في الجزائر، لقلة خبرتها في هذا الشق، وغياب المختصين والخبراء القادرين على تشخيص الجريمة قبل عرضها على المحكمة للفصل فيها، وعدم تهيئة الأسس التقنية الكفيلة بتصنيف درجات هذه الجرائم وحدة أضرارها قبل إصدار العقوبة، هذا فضلاً عن غياب التواصل الدائم بين القضاء والمختصين في الاتصالات، ما أفرز شبه تذبذب وغموض في شأن العقوبات الدقيقة في مثل هذه الجرائم (44).

6- **خاتمة**

وفي ختام هذه الورقة العلمية، نشير إلى ما قاله الأمريكي" ايريك هولدر Eric Holder" الإنترنيت و الحاسبات الآلية جلبت منافع جمة للمجتمع، متضمنة حرية عظمى للتعبير وللنمو الاقتصادي، ولكن يجب أن ندرك أنه ونتيجة لتزايد اعتماد مجتمعاتنا على التكنولوجيا فإن جهات التحقيق والمدعين والعاملين يواجهون على كافة المستويات (دولية – فيدرالية – محلية) تحديات فريدة " (45).

ويشير "جيمس روبنسون " James Robinnso " إلى هذه التحديات وهي ثلاث تحديات:

أ– تحديات تقنية : وتتمثل في صعوبة تحديد مصدر اعتداء مرتكبي جرائم الحاسب الآلي لأن المجرم الإلكتروني عادة يحاول ترك أمر تتبعه مستحيلاً، ومع تزايد التطور التكنولوجي ظهرت تقنيات جديدة لإخفاء الأثر، إضافة إلى أن شبكة الإنترنيت تزيد الأمر تعقيداً، لأن المجرمين بواسطتها يتمكنون من إخفاء هويتهم و يستطيعون ارتكاب جرائمهم من أماكن بعيدة و بمعاونة شركاء لهم من بلدان أخرى وبإجراء اتصالات مختلفة لتضليل لجان التحقيق (46).

ب– تحديات قانونية : تختلف التشريعات في معالجتها للجرائم الإلكترونية، فنجد بعض الدول وإن وضعت منظومة تشريعية لمواجهة الجريمة المعلوماتية إلا أن الواقع أثبت قصورها في العديد من المرات بسبب التطور السريع للجريمة المعلوماتية، إضافة إلى هذا عدم تجريم الدول للجرائم المعلوماتية يجعل من الصعب و المستحيل تتبع المجرمين وضبطهم.

ج– تحديات فنية : في أغلب الحالات يتفوق المجرم المعلوماتي عن رجال التحقيق ورجال القضاء، وهذا مرده إلى المعرفة الكبيرة بتقنية المعلومات بالنسبة للمجرم المعلوماتي، بينما بالمقابل نجد أن رجال التحقيق ورجال القضاء يفتقرون على الخبرة والمعرفة الفنية في هذا النوع من الإجرام، الأمر الذي يزيد من صعوبة التحقيق و إثبات الجرائم.

هذا فضلاً عن وجود صعوبات أخرى في مجال مكافحة الجريمة الإلكترونية كمحدودية الاتفاقيات الدولية عن تبادل المعلومات حول هذه الجريمة، وغياب العقوبة الرادعة، وضعف التعاون مع القطاع الخاص والشركات المزودة لخدمة الإنترنت والاتصالات، إضافة إلى تسارع التطور التقني في هذا النمط المميز من الجرائم.

وتذليلاً لهذه التحديات هناك ما يمكن القيام به على المستوى الوطني، كوضع منظومة تشريعية كفيلة بمحاربة الجريمة المعلوماتية، بالإضافة إلى وضع إستراتيجية وطنية شاملة لحماية أمن المعلومات و مواجهة الهجمات الإلكترونية، بالإضافة إلى تكوين الكادر المؤهل في كل التخصصات للتعامل مع هذا النوع من الجرائم، وفي الأخير فإن هذه الجهود لن تتكل بالنجاح إن لم تتحد الجهود على المستوى الدولي لمواجهة هذه الظاهرة.

كما توصلنا من خلال هذا البحث إلى النتائج و المقترحات التالية :

1– عدم قيام بعض الدول العربية بسن قوانين خاصة بالجرائم المعلوماتية، بالرغم من تزيد انتشارها في السنوات الأخيرة، لذلك على هذه الدول تدارك هذا النقص حتى يمكنها متابعة ومعاقبة مرتكبي هذه الجرائم استناداً إلى مبدأ الشرعية الجنائية ومواكبة التطور الحاصل في هذا المجال.

2– على الدول العربية توسيع اختصاصها القضائي في مجال الجرائم الإلكترونية استناداً إلى مبدأ الشخصية و العينية وعدم اقتصارها على مبدأ الإقليمية المعروف في النظم والقوانين الجنائية الداخلية، والاستفادة من تجربة الولايات المتحدة الأمريكية وبريطانيا وفرنسا في هذا الشأن.

3– إبرام اتفاقيات عربية وإقليمية لمكافحة الجرائم المعلوماتية، وتوثيق أواصر التعاون فيما بينها في هذا المجال.

4– التفكير في إنشاء شرطة جنائية عربية على غرار الشرطة الجنائية الدولية "الأنتربول"، والشرطة الجنائية الأوروبية "الإيربول" مكونة من خبراء عرب في المجال الشرطي والقانوني والمعلوماتي وغيرهم، وتكليفها بالبحث ومتابعة والتحقيق في الجرائم المعلوماتية التي تحدث في البلدان العربية أو تصيب مصالحها بضرر.

5– قيام الدول بتدريب قضاتها، وخاصة قضاة التحقيق والنيابة العامة على تكنولوجيا المعلومات والاتصالات بغية تسهيل مهامها في مجال البحث والتحقيق في الجرائم الإلكترونية وإثباتها.

6– الاعتداد بوسائل الإثبات الجنائي الحديثة وفي مجال الكشف عن الجرائم المعلوماتية ومرتكبيها بالمستندات الإلكترونية، البريد الإلكتروني وغيرها والنص عليها في نصوص قانوني واضحة وصريحة.

7– إنشاء معاهد وفتح تخصصات في الجامعات تعني بالأمن المعلوماتي، والتدريب فيه ومواكبة كل التطورات الحاصلة هذا المجال.

8– أصبحت دول العربية أكثر وعياً وإدراكاً لحجم المخاطر الناجمة عن الجرائم الإلكترونية، ومع تبدل المشهد الأمني ونشوء تحديات جديدة في هذا الإطار، فإنه بات يتعين على هذه الدول مواصلة صياغة الخطط والإستراتيجيات الكفيلة بتعزيز الوعي لدى الأفراد والمؤسسات والحكومات، وإعدادهم بالشكل الأمثل للتصدي لهذه الجرائم.

9- وتطبيقاً لمبدأ "الوقاية خير من العلاج " على الدول العربية تطبيق ما يسمى "بالأمن الإلكتروني " باستعمال تقنيات معلوماتية متطورة والعمل على تحديثها و مراقبتها، وتعزيز سبل التعاون بين هذه الدول في هذا المجال.

المراجع

[1] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنيت، دار الفكر العربي الإسكندرية طبعة 2007، ص 35.

[2] عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنيت، دار الكتب والوثائق المصرية، ص 43 – 45.

[3] معلومات مستقاة من الموقع الإلكتروني، http:/elaph.com/web/news.

[4] منى شاكر فراج العسبلي، تأثير الجريمة الإلكترونية على النواحي الإقتصادية، مقال منشور على الموقع الإلكتروني لمركز التميز للأمن المعلوماتي، www.coeia.edu.sa

[5] أنظر عبد الله الغفيص، مقال بعنوان تراجع معدل الإنفاق العالمي على تقنية المعلومات بنسبة 5.5 % خلال العام 2015، منشور بتاريخ 21 يوليو 2015، على الموقع الإلكتروني التالي: http://www.n1t1.com

[6] سامي علي حامد عياد، المرجع السابق، ص 42.

[7] المرجع نفسه.

[8] محمد أمين الشوابكة، جرائم الحاسوب والإنترنيت، دار الثقافة عمان الأردن، الطبعة الأولى، ص 9.

[9] راجع صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري بتيزي وزو، الجزائر، 2013، ص 16.

[10] د/ محمد حماد مرهج الهيتي، جرائم الحاسوب – ماهيتها. موضوعها. أهم صورها. والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع، عمان الأردن، الطبعة الأولى 2006، ص 211.

[11] رستم هشام، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الأمن والقانون دبي، العدد الثاني سنة 1999.

[12] راجع صغير يوسف، المرجع السابق، نفس الصفحة.

[13] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت، دار الكتب القانونية طبعة 2002، ص 46.

[14] راجع صغير يوسف، المرجع السابق، ص 19 – 20.

[15] د/ محمد حماد مرهج الهيتي، المرجع السابق، ص 218.

[16] راجع الموقع الإلكتروني التالي : http://drot7.blogspot.com/2013/11/blog-post_9658.html

[17] د أسامة أبو الحجاج، دليلك الشخصي إلى الإنترنيت، نهضة مصر – القاهرة – طبعة 1998، ص 20.

[18] د علي جبار الحسيناوي، جرائم الحاسوب والإنترنيت، دار اليازوري العلمية للنشر والتوزيع، عمان الأردن الطبعة الأولى 2009، ص 163.

[19] محمد عبد الله المنشاوي، جرائم الإنترنيت من منظور شرعي وقانوني، مكة المكرمة 1/ 11/ 2013 من خلال الموقع الإلكتروني: Mohamed@minshawi.com

[20] أنظر هذه الإحصائيات في مقال بعنوان الجرائم الإلكترونية تنتشر في الأردن منشور بتاريخ 09/ 12/ 2014 على الموقع الإلكتروني التالي: http://albosala.com

[21] معلومات مستقاة من الوقع الإلكتروني التالي : http://www.aldaawa.com/?p=7833

[22] د علي جبار الحسيناوي، المرجع السابق، ص 164.

[23] محمود أحمد عباينة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، طبعة 2009، ص 145.

[24] راجع الموقع الإلكتروني : http:www.usdoj.gov/criminal/cybercrime/iplaws.html.page3of5

[25] أ. د موسى مسعود ارحومة، مقال بعنوان الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون، طرابلس، 2009، ص 19.

[26] المرجع نفسه، ص 11.

[27] محمود أحمد عبابنة، المرجع السابق، ص 151.
[28] موسى مسعود ارحومة، المرجع السابق، ص 11.
[29] محمد عبد الله المنشاوي، المرجع السابق.
[30] أ. د موسى مسعود ارحومة، المرجع السابق، ص 19.
[31] المرجع نفسه.
[32] عبد الله مجيد، الجريمة الإلكترونية تكلف العالم 400 مليار دولار سنوياً، مقال منشور بتاريخ 10/ 06/ 2014 على الموقع الإلكتروني التالي : http://elaph.com
[33] محمد أمين الشوابكة، المرجع السابق، ص 80.
[34] منى شاكر فراج العسبلي، المرجع السابق.
[35] المرجع نفسه.
[36] أنظر هذه الإحصائيات في مقال بعنوان الجرائم الإلكترونية تنتشر في الأردن منشور بتاريخ 09/ 12/ 2014 على الموقع الإلكتروني التالي : http://albosala.com
[37] محمد عبد الله المنشاوي، المرجع السابق.
[38] مقال بعنوان الجرائم الإلكترونية تنتشر في الأردن، منشور بتاريخ 09/ 12/ 2014 على الموقع الإلكتروني التالي: http:albosala.com
[39] د علي جبار الحسيناوي، المرجع السابق، ص 177 – 178.
[40] راجع الموقع الإلكتروني التالي : http:www.djazairess.com/alfadjr/71333.
[41] راجع الموقع الإلكتروني التالي : http://www.essalamonline.com
[42] المديرية العامة للأمن الوطني الجزائري، مقال بعنوان الجريمة الإلكترونية، المديرية العامة للأمن الوطني تعالج أكثر من 380 قضية خلال السداسي الأول 2013، منشور على الموقع الإلكتروني التالي :http://www.ennaharonline.com/ar/algeria_news
[43] راجع صغير يوسف، المرجع السابق، ص 108 – 112.
[44] مقال خاص برئيس اللجنة الاستشارية لحقوق الإنسان في الجزائر، بعنوان تطبيق العقوبات في قضايا الجريمة الإلكترونية صعب في الجزائر و 160 مليار دولار سنوياً مكاسب عصابات الجريمة المنظمة عبر الإنترنت، منشور بتاريخ 24 – 1- 2014، على الموقع الإلكتروني التالي : http://www.djazairess.com
[45] محمود أحمد عبابنة، المرجع السابق، ص 146.
[46] المرجع نفسه.